UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/482,840	01/13/2000	Marcus Peinado	MSFT-0109/127334.9	7581

7590 01/16/2003

Steven H Meyer
WOODCOCK WASHBURN KURTZ MACKIEWICZ & NORRIS LLP
One Liberty Place
46th Floor
Philadelphia, PA 19103

EXAMINER
NGUYEN, CUONG H

ART UNIT	PAPER NUMBER
3625	

DATE MAILED: 01/16/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No. 09/482,480	Applicant(s) Peinado et al.
Examiner Cuong H. Nguyen	Art Unit 3625

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *8/19/2002 (the supp. IDS)* .

2a) ☐ This action is **FINAL.** 2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11; 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-181* is/are pending in the application.

4a) Of the above, claim(s) *1-105* is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *106-181* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claims _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are objected to by the Examiner.

11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved.

12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

13) ☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

a) ☐ All b) ☐ Some* c) ☐ None of:

1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

*See the attached detailed Office action for a list of the certified copies not received.

14) ☒ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

15) ☒ Notice of References Cited (PTO-892)

16) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

17) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s). _____

18) ☐ Interview Summary (PTO-413) Paper No(s). _____

19) ☐ Notice of Informal Patent Application (PTO-152)

20) ☐ Other:

DETAILED ACTION

1. This Office Action is the answer to the communication received on 8/19/2002 (the Supp. IDS).

2. Claims 106-181 are pending in this application

Drawings

3. This application has been filed with formal drawings which currently are acceptable for examining purposes.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C.§ 103(a) which forms the basis for all obviousness rejections set forth in this Office Action:

> *(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.*

4. Claims **106-181** are rejected under 35 U.S.C.§ 103(a) as being unpatentable over **Krishnan**, (US Pat.6,073,124), in view of **Stefik** (US Pat. 5,715,403), and further in view of the Official Notice.

First of all, the examiner submits that a DRM obviously having a structure/"box" with encryption/decryption keys inside is very obvious (as claiming a digital right management having encryption/decryption keys (or a public/private key pair which is similar to encryption/decryption keys)).

A. Claim **106**: In a digital rights management (DRM) system, a method of obtaining a structure having encryption/decryption keys, comprising:

- requesting encryption/decryption keys;
- generating, unique public/private key pair (or encryption/decryption keys);
- delivering encryption/decryption keys; and
- installing encryption/decryption keys in said DRM system.

All above steps are merely communications (requesting/ generating/transmitting/receiving/installing encryption/decryption keys) between 2 parties to utilize encryption/decryption keys; **Stefik** obviously suggests that communication (see at least **Stefik**, "*Transactions require that there be some communication between repositories. Communication between repositories occurs in units termed as messages. Because the communication line is assumed to be unsecure, all communications with repositories that are above the lowest security class are encrypted utilizing a public key encryption technique. Public key encryption is a well known technique in the encryption arts. The term key refers to a numeric code that is used with encryption and decryption algorithms. Keys come in pairs, where "writing keys" are used to encrypt data and "checking keys" are used to decrypt data. Both writing and checking keys may be public or private. Public keys are those that are distributed to others. Private keys are maintained in confidence*"; *and*

"*An encryption technique used for secure transmission of messages on a communication channel. Key pairs are used for the encryption and decryption of messages. Typically one key is referred to as the public key and the other is the private key. The keys are inverses of each other from the perspective of encryption. Restated, a*

digital work that is encrypted by one key in the pair can be decrypted only by the other."). The examiner submits that the contents of this claim are also notoriously well-known in computer-related art: a system, wherein a content server distributes the digital content in an encrypted form, and wherein the DRM system includes a structure for performing decryption and encryption functions for such DRM system; and wherein the structure includes a unique public/private key pair (for performing the decryption and encryption functions).

The Official Notice are taken that the following underlined features were known before the priority date of this pending application:

B. Claim **107**: The method of claim 106 wherein the DRM system has a previously installed structure relating to (encryption/decryption keys) prior to the requesting step, the method further comprising determining prior to the requesting step that the previously installed structure is non-unique.

The examiner submits that it is obvious to one with skill in the art to change the order of required steps in a procedure because the order is still logic/reasonable/making sense. It would be obvious to artisans that a step of "determining prior to the requesting step that the previously installed structure is non-unique" have been known to be done to avoid any possible error (e.g., **Stefik** suggests that "Assuming that the repository is not

on the hotlist, the repository identification needs to be verified. In other words, repository-2 needs to validate that the repository on the other end is really repository-1. This is termed performance testing and is performed in order to avoid invalid access to the repository via a counterfeit repository replaying a recording of a prior session initiation between repository-1 and repository-2. Performance testing is initiated by repository-2 generating a performance message, step 1609. The performance message consists of a nonce, the names of the respective repositories, the time and the registration identifier received from repository-1. A nonce is a generated message based on some random and variable information (e.g. the time or the temperature.) The nonce is used to check whether repository-1 can actually exhibit correct encrypting of a message using the private keys it claims to have, on a message that it has never seen before. The performance message is encrypted using the public key specified in the registration message of repository-1. The performance message is transmitted to repository-1, step 1610, where it is decrypted by repository-1 using its private key, step 1611. Repository-1 then checks to make sure that the names of the two repositories are correct, step 1612, that the time is accurate, step 1613 and that the registration identifier corresponds to the one it sent, step 1614. If any of these tests fails, the transaction is terminated per step 1616. Assuming that the tests are passed, repository-1 transmits the nonce to repository-2 in the clear, step 1615. Repository-2 then compares the received nonce to the original nonce, step 1617. If they are not identical, the registration transaction terminates in an error per step 1618. If they are the same, the registration transaction has successfully completed.").

C. Claim **108**: The method of claim 106 wherein the DRM system has a previously installed structure prior to the requesting step, the method further comprising determining prior to the requesting step that the previously installed structure is not current.

The examiner submits that this claimed step is obviously analogous to claim **107**'s limitation because a step of "checking if encryption/decryption key is unique" is similar to "checking to see if said keys are current or not"; therefore, similar rationale and reference are applied.

D. Claim **109**: The method of claim 106 with requesting the structure (a unique public/private key pair (for performing the decryption and encryption functions)) by way of a network connection to a server (this feature is inherent in **Stefik**'s patent, see Fig.19).

E. Claim **110**: The method of claim 109 wherein the requesting step comprises requesting the structure by way of an Internet connection to the structure server (this feature is inherent in **Stefik**'s patent, see Fig.19).

F. Claim **111**: The method of claim 106 wherein the DRM system has a first previously installed structure prior to the requesting step, the first previously installed structure having a public/private key pair different from the public/private key pair of the generated structure, and wherein the generating step includes providing the generated structure with the public/private key pair of the first previously installed structure (e.g., see **Ginter** et al., "An important aspect of adding or modifying content is the choice of encryption/decryption keys and/or other relevant aspects of securing new or altered content. The provider may

specify in their method(s) associated with these processes a technique or techniques to be used for creating and/or selecting the encryption/decryption keys and/or other relevant aspect of securing new and/or altered content. For example, the provider may include a collection of keys, a technique for generating new keys, a reference to a load module that will generate keys, a protocol for securing content, and/or other similar information." Or see **Ginter** et al., "Another important implication is the management of new keys, if any are created and/or used. A provider may require that such keys and reference to which keys were used must be transmitted to the provider, or she may allow the keys and/or securing strategy to remain outside a provider's knowledge and/or control. A provider may also choose an intermediate course in which some keys must be transmitted and others may remain outside her knowledge and/or control.").

G. Claim **112**: The method of claim 111 wherein the DRM system had a second previously installed structure prior to having the first previously installed structure, the second previously installed structure having a public/private key pair different from the public/private key pair of the first previously installed structure and also different from the public/private key pair of the generated structure, and wherein the generating step further includes providing the generated structure with the public/private key pair of the second previously installed structure.

The examiner submits that this claimed step is obviously analogous to claim **111's** limitation because

analogous repetition of a step is claimed; therefore, similar rationale and reference are applied.

H. Claim 113: The method of claim 106 wherein the generating step includes providing the generated structure with an identifier (e.g., **Stefik** suggests an analogous step using provided identifier "The registration transaction between two repositories is described with respect to FIGS. 16 and 17. The steps described are from the perspective of a "repository-1" registering its identity with a "repository-2". The registration must be symmetrical so the same set of steps will be repeated for repository-2 registering its identity with repository-1. Referring to FIG. 16, repository-1 first generates an encrypted registration identifier, step 1601 and then generates a registration message, step 1602. A registration message is comprised of an identifier of a master repository, the identification certificate for the repository-1 and an encrypted random registration identifier. The identification certificate is encrypted by the master repository in its private key and attests to the fact that the repository (here repository-1) is a bona fide repository. The identification certificate also contains a public key for the repository, the repository security level and a timestamp (indicating a time after which the certificate is no longer valid.) The registration identifier is a number generated by the repository for this registration. The registration identifier is unique to the session and is encrypted in repository-1's private key. The registration identifier is used to improve security of authentication by detecting certain kinds of communications based attacks. Repository-1 then transmits the registration message to repository-2, step 1603."

I. Claim **114**: The method of claim 113 wherein the generating step includes providing the generated structure with a version number. The examiner submits that "a version number" is analogous to "something to identify"; and **Stefik**'s patent suggests that feature.

J. Claim **115**: The method of claim 106 wherein the generating step includes providing the generated structure with a digital certificate (e.g., this feature is obviously suggested in **Stefik**'s patent: "This version makes it possible to hold distributors accountable in some way for the sales and support of the work, by controlling the distribution of certificates that enable distributors to legitimately charge fees and copy owners to make copies.").

K. Claim **116**: The examiner submits that this claim's limitation is similar to claim 115's limitation; therefore, similar rationale & reference are applied.

L. Claim **117**: The method of claim 106 wherein the generating step includes encrypting a private key (e.g. see Ginter et al. "If public-key cryptography is used as the basis for external communication with PPE 650, then a master key is required during the PPE Public-key pair certification process. This master key may be, for example, a private key used by the manufacturer or VDE administrator to establish the digital certificate (encrypted public key and other information of the PPE), or it may, as another example, be a private key used by a VDE administrator to encrypt the entries in a certification repository. Once

certification has occurred, external communications between PPEs 650 may be established using the certificates of communicating PPEs." .

M. Claim **118**: The examiner submits that this claim's limitation is similar to claim 117's limitation; therefore, similar rationale & reference are applied.

N. Claim **119**: The method of claim 106 wherein the generating step includes associating the generated structure with a computing device. This is very obvious with artisans because the environment here is computer networking.

O. Claim **120**: The method of claim 119 wherein the requesting step includes providing unique information to said computing system, and generating the structure based on provided information (e.g., see **Ginter** et al. "An important part of VDE provided by the present invention is the core secure transaction control arrangement, herein called an SPU (or SPUs), that typically must be present in each user's computer, other electronic appliance, or network. SPUs provide a trusted environment for generating decryption keys, encrypting and decrypting information, managing the secure communication of keys and other information between electronic appliances (i.e., between VDE installations and/or between plural VDE instances within a single VDE installation), securely accumulating and managing audit trail, reporting, and budget information in secure and/or non-secure non-volatile memory, maintaining a secure database of control information management instructions, and providing a secure environment for performing certain other control and administrative functions."; or see **Ginter** et al.:

"An important aspect of adding or modifying content is the choice of encryption/ decryption keys and/or other relevant aspects of securing new or altered content. The provider may specify in their method(s) associated with these processes a technique or techniques to be used for creating and/or selecting the encryption/decryption keys and/or other relevant aspect of securing new and/or altered content. For example, the provider may include a collection of keys, a technique for generating new keys, a reference to a load module that will generate keys, a protocol for securing content, and/or other similar information.".

P. Claim **121**: The method of claim 119 wherein the DRM system is a first DRM system, wherein the generating step includes associating the generated structure with computing devices. The examiner submits that encryption/decryption (a box that contains encryption/decryption) keys have been known by artisans to be associated with computing devices (e.g., ID number .etc.) for identification purposes.

5. Re. to Claims **122, 138, 152, 168**: These claims' limitations are obviously analogous to limitation(s) of claim **106**. Therefore, similar rationale and references set forth are applied for rejection(s) under 35 U.S.C.§ 103(a).

6. Re. to Claims **139, 155, 160, 125**: These claims' limitation(s) are obviously analogous to limitation(s) of claim **109**. Therefore, similar rationale and references set forth are applied for rejection(s) under 35 U.S.C.§ 103(a).

7. Re. to Claims **140, 156, 170, 126**: These claims' limitation(s) are obviously analogous to limitation(s) of claim **110**. Therefore, similar rationale and references set forth are applied for rejection(s) under 35 U.S.C.§ 103(a).

8. Re. to Claims **141, 157, 171, 127**: These claims' limitation(s) are obviously analogous to limitation(s) of claim **111**. Therefore, similar rationale and references set forth are applied for rejection(s) under 35 U.S.C.§ 103(a).

9. Re. to Claims **142, 158, 172, 128**: These claims' limitation(s) are obviously analogous to limitation(s) of claim **112**. Therefore, similar rationale and references set forth are applied for rejection(s) under 35 U.S.C.§ 103(a).

10. Re. to Claims **143, 159, 173, 129**: These claims' limitation(s) are obviously analogous to limitation(s) of claim **113**. Therefore, similar rationale and references set forth are applied for rejection(s) under 35 U.S.C.§ 103(a).

11. Re. to Claims **130, 144, 160, 174**: These claims' limitation(s) are obviously analogous to limitation(s) of claim **114**. Therefore, similar rationale and references set forth are applied for rejection(s) under 35 U.S.C.§ 103(a).

12. Re. to Claims **131, 145, 151, 175**: These claims' limitation(s) are obviously analogous to limitation(s) of claim **115**. Therefore, similar rationale and references set forth are applied for rejection(s) under 35 U.S.C.§ 103(a).

13. Re. to Claims **146, 162, 176, 132**: These claims' limitation(s) are obviously analogous to limitation(s) of

claim **116**. Therefore, similar rationale and references set forth are applied for rejection(s) under 35 U.S.C.§ 103(a).

14. Re. to Claims **133, 147, 163, 177**: These claims' limitation(s) are obviously analogous to limitation(s) of claim **117**. Therefore, similar rationale and references set forth are applied for rejection(s) under 35 U.S.C.§ 103(a).

15. Re. to Claims **134, 148, 164, 178**: These claims' limitation(s) are obviously analogous to limitation(s) of claim **118**. Therefore, similar rationale and references set forth are applied for rejection(s) under 35 U.S.C.§ 103(a).

16. Re. to Claims **149, 165, 179, 135**: These claims' limitation(s) are obviously analogous to limitation(s) of claim **119**. Therefore, similar rationale and references set forth are applied for rejection(s) under 35 U.S.C.§ 103(a).

17. Re. to Claims **136, 150, 166, 180**: These claims' limitation(s) are obviously analogous to limitation(s) of claim **120**. Therefore, similar rationale and references set forth are applied for rejection(s) under 35 U.S.C.§ 103(a).

18. Re. to Claims **137, 151, 167, 181**: These claims' limitation(s) are obviously analogous to limitation(s) of claim **121**. Therefore, similar rationale and references set forth are applied for rejection(s) under 35 U.S.C.§ 103(a).

19. Re. to Claims **153, 123**: These claims' limitation(s) are obviously analogous to limitation(s) of claim **107**. Therefore, similar rationale and references set forth are applied for rejection(s) under 35 U.S.C.§ 103(a).

20. Re. to Claims **154, 124**: These claims' limitation(s) are obviously analogous to limitation(s) of claim **108**. Therefore, similar rationale and references set forth are applied for rejection(s) under 35 U.S.C.§ 103(a).

The examiner submits that all pending claimed limitations are inherent/well-known in a computer system, because these claimed limitations are old that they are easily recognized to be components of a computer system and said components would perform claimed tasks/steps; cited prior art's limitations are not necessary spelled-out exactly claimed languages, because cited prior art is also directed to a similar process/system for transferring money from a safe. **Stefik** or submitted IDS references are not limited to the described embodiments in their documents. It is reasonable that various modifications of the described suggestions of the cited prior art would be apparent to those skilled in the art without departing from the scope and spirit of their disclosures. It should be understood that their suggestions should not be unduly limited to specific embodiments in said disclosures.

It would have been obvious to one of ordinary skill in the art at the time of invention to implement the system of **Stefik** with suggestions readily available in the art submitted in the IDS and in view of the Official Notice, because these information would improve communications and

give different levels of security for a digital right management system.

Conclusion

22. Claims **106-181** are rejected.

23. These references are considered pertinent to applicants' disclosure.

- **Krishnan,** (US Pat.6073124 - 6/06/2000), Method and system for securely incorporating electronic information into an online purchasing application

- **Stefik,** (US Pat. 5,715,403), discloses about a system for controlling the distribution and use of digital works having attached usage rights where the usage rights are defined by a usage rights grammar.

- **Stefik** et al., (US Pat. 5,629,980), discloses about a system for controlling the distribution and use of digital works.

- **Van Wie** et al., (US Pat. 5,943,422), discloses about a steganographic techniques for securely delivering electronic digital rights management control information over insecure communication channels.

- **Ginter** et al., (US Pat. 5,982,891), discloses about a system and a method for secure transaction management and electronic rights protection.

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Cuong

H. Nguyen whose telephone number is 703-305-4553 The examiner can normally be reached on Mon.-Fri. from 7:00 AM to 3:15 PM (EST).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ms. Wynn Coggins, can be reached on (703)308-1344.

Any response to this action should be mailed to:

Amendments

Commissioner of Patents and Trademarks
Washington D.C. 20231

or faxed to: (703)305-7687 [Official communications; including After Final communications labeled "Box AF"]

703-746-5572 (RightFax) Informal/Draft communications, labeled "PROPOSED" or "DRAFT"]

Hand delivered responses should be brought to Crystal Park 5, 2451 Crystal Drive, Arlington, VA, 7th floor receptionist.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Receptionist whose telephone number is (703)308-1113.

Cuong Nguyen
Primary Examiner
Jan. 13, 2003